Deutscher Bundestag **Drucksache 19/11478**

19. Wahlperiode 10.07.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Benjamin Strasser, Stephan Thomae, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/11133 –

Wanzen im Wohnzimmer – Überwachung durch Sprachassistenten und smarte Geräte

Vorbemerkung der Fragesteller

Weltweit steigt die Zahl digital vernetzter Geräte. Intelligente Sprachassistenten wie Alexa oder smarte Haushaltsgeräte unterstützen auch in Deutschland immer mehr Menschen in ihrem Alltag. Prognosen zufolge wird bereits in fünf Jahren jeder Privathaushalt mit rund 500 vernetzten Geräten ausgestattet sein (www.tuv.com/de/deutschland/ueber_uns/presse/meldungen/newscontentde_380800.html). Die Masse an digital vernetzten Geräten erzeugt ebenso große Mengen an verfügbaren Daten. Bisher stellte sich insbesondere die Frage nach dem Schutz dieser in privatesten Lebensbereichen entstandenen Daten vor illegalen Zugriffen.

Nach Plänen der Innenminister von Bund und Ländern sollen künftig jedoch auch die Strafverfolgungsbehörden Zugriff auf entsprechende Daten erhalten. Das Innenministerium Schleswig-Holsteins hat eine entsprechende Beschlussvorlage für die Innenministerkonferenz, die vom 12. bis 14. Juni in Kiel stattfindet, formuliert (vgl. www.zdf.de/nachrichten/heute/innenminister-vorstoss-ermittler-sollen-zugriff-auf-daten-aus-smarten-geraeten-erhalten-100.html). Ein Sprecher des Bundesministerium des Innern, für Bau und Heimat bestätigte, dass es für eine effektive Kriminalitätsbekämpfung sehr wichtig sei, dass den Sicherheitsbehörden von Bund und Ländern auch auf diesen Geräten gespeicherte Daten nicht verschlossen blieben (vgl. www.spiegel.de/netzwelt/netzpolitik/justizministerium-warnt-ermittler-vor-zugriff-auf-sprachassistenten-wie-alexa-und-siri-a-1271089.html). Das Bundesministerium der Justiz und für Verbraucherschutz verwies hingegen darauf, dass der Schutz der persönlichsten Lebensbereiche und die Freiheit jedes Beschuldigten, sich nicht selbst zu belasten, Grenzen setze, die nicht umgangen werden dürften (vgl. www.heise.de/newsticker/meldung/Justizministerium-warnt-vor-Zugriff-auf-Daten-von-Alexa-Co-4441123.html).

Aus Sicht der Fragesteller steht dieser potentielle Zugriff auf Millionen entsprechender Geräte allein in Deutschland einen inakzeptablen Eingriff in die Bürgerrechte von Millionen unschuldiger Bürger dar. Nicht nur würden die Ermittlungsbehörden im Falle des Zugriffs einen tiefreichenden Einblick in den priva-

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 9. Juli 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

ten Kernbereich der Bürger erhalten. Auch bereits die Angst, dass der Staat unbemerkt mithören könnte, schränkt die individuelle Freiheit erheblich ein. So hatte schon das Bundesverfassungsgericht (BVerfG) in seinem Urteil bezüglich der Verfassungsmäßigkeit der Vorratsdatenspeicherung betont, dass durch die vom Bürger unbemerkte Verwendung von Daten „ein Gefühl des ständigen Überwachtwerdens“ hervorgerufen werden könne (vgl. BVerfG, Urteil des Ersten Senats vom 2. März 2010 – 1 BvR 256/08 – Rn. 1 – 345). Überdies ist fraglich, welcher Wert den Daten als Beweismittel in einem Gerichtsverfahren überhaupt zugesprochen werden kann, angesichts der Gefahr der Manipulation durch illegale Zugriffe.

Vorbemerkung der Bundesregierung

Bei den beschriebenen vernetzten Geräten wie den intelligenten Sprachassistenten (z. B. Alexa) oder auch smarten Haushaltsgeräten handelt es sich nicht um eine Geräteklasse, die von der bisherigen Gesetzgebung nicht umfasst ist. Die in der Kleinen Anfrage bezeichneten Geräte stellen vielmehr lediglich eine Form des informationstechnischen Systems dar, für die zum jetzigen Zeitpunkt kein spezifischer strafprozessualer Regelungsbedarf ersichtlich ist. Da die bestehenden gesetzlichen Regelungen technikneutral und geräteunabhängig formuliert sind, erfassen sie diese Geräteklasse bereits.

1. Wie erklärt die Bundesregierung den in der Vorbemerkung der Fragesteller genannten öffentlichen Dissens zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Bundesministerium der Justiz und für Verbraucherschutz zur Überwachung von Technologien wie smarten Geräten, Sprachassistenten etc.?

Ein Dissens besteht aus Sicht der Bundesregierung nicht.

2. Hat die Bundesregierung inzwischen eine konsentierte Position zu der Thematik, und wenn ja, welche?

Es wird auf die Antwort zu Frage 1 verwiesen. Im Übrigen ist die Haltung der Bundesregierung zur Anwendung der einzelnen Eingriffsnormen aus den nachstehenden Antworten ersichtlich.

3. Unter welchen Voraussetzungen und aufgrund welcher bereits bestehenden rechtlichen Grundlage ist ein Zugriff auf die Daten von vernetzten Geräten durch die Strafverfolgungsbehörden zulässig?

Auf die einzelnen Darstellungen in den Antworten zu den der Fragen 4 bis 9 wird verwiesen.

4. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur Beschlagnahme gemäß §§ 94 ff. der Strafprozessordnung (StPO) möglich?

§ 94 StPO erlaubt sowohl die Beschlagnahme von Geräten als auch die Beschlagnahme von Daten. Vernetzte Geräte und die hierauf gespeicherten Daten sind hiervon nicht ausgenommen. Die Beschlagnahme ist als offene Maßnahme ausgestaltet.

5. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur Quellen-Telekommunikationsüberwachung gemäß § 100a StPO möglich?

Soweit über das vernetzte Gerät Telekommunikation erfolgt, findet § 100a StPO Anwendung. Eine Quellen-Telekommunikationsüberwachung kann in diesem Fall nur unter den in § 100a StPO geregelten Voraussetzungen erfolgen.

6. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur Onlinedurchsuchung gemäß § 100b StPO möglich?

Soweit es sich bei dem vernetzten Gerät um ein informationstechnisches System handelt, finden die Bestimmungen von § 100b StPO Anwendung. Ein Eingriff in das informationstechnische System und die Erhebung von Daten hieraus darf nur erfolgen, soweit die engen in § 100b StPO geregelten Eingriffsvoraussetzungen vorliegen.

7. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur akustischen Wohnraumüberwachung gemäß § 100c StPO möglich?

§ 100c StPO ermöglicht unter den dort vorgesehenen Voraussetzungen die Aufzeichnung des nichtöffentlich gesprochenen Wortes des Beschuldigten. Zu diesem Zweck dürfen technische Mittel eingesetzt werden. § 100c StPO regelt jedoch nicht den Zugriff auf informationstechnische Systeme. Der Zugriff auf informationstechnische Systeme ist allein unter den Voraussetzungen und auf der Grundlage von § 100b StPO zulässig.

8. Inwieweit und insbesondere in welcher Konstellation ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte auf Grundlage der Regelungen zur Durchsicht elektronischer Aufzeichnungen gemäß § 110 StPO möglich?

Für die Durchsicht von im Rahmen der Durchsuchung aufgefundenen Datenträgern gilt § 110 Absatz 1 StPO, so dass ein lokales Speichermedium auf dieser Grundlage durchgesehen werden kann. § 110 Absatz 3 Satz 1 StPO regelt darüber hinaus die Erstreckung der Durchsicht auf verbundene Speichermedien.

Erfolgt im Rahmen einer Durchsuchung eine Durchsicht eines elektronischen Speichermediums, so kann diese auf ein hiervon räumlich getrenntes Speichermedium erstreckt werden. Ist das vernetzte Gerät daher ein Speichermedium, das mit einem anderen Speichermedium verbunden ist, findet § 110 Absatz 3 StPO Anwendung.

9. Wie kann aus Sicht der Bundesregierung sichergestellt werden, dass der Schutz des Kernbereichs privater Lebensgestaltung im Rahmen der genannten Eingriffe gewährleisten wird, insbesondere angesichts des Umstandes, dass sich die vernetzten Geräte oftmals nicht vollständig von den Behörden steuern lassen (bitte nach einzelnen Eingriffsgrundlagen aufschlüsseln)?

Mit § 100d StPO wurde durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl I, S. 3202 – 3213) eine Vorschrift geschaffen, die bei der Vornahme der Ermittlungsmaßnahmen nach den §§ 100a bis 100c StPO den Schutz des Kernbereichs privater Lebensgestaltung sicherstellt.

10. Inwiefern müssten bestehende Regelungen ergänzt oder neue rechtliche Grundlagen geschaffen werden, um einen Zugriff auf die Daten von vernetzten Geräten durch die Strafverfolgungsbehörden zu ermöglichen?

In der Strafprozessordnung stehen bereits geeignete Rechtsgrundlagen für den Zugriff auf die Daten von vernetzten Geräten zur Verfügung.

11. Inwieweit ist aus Sicht der Bundesregierung der Zugriff auf vernetzte Geräte mit der Quellen-Telekommunikationsüberwachung gemäß § 100a StPO und dem Einsatz der Onlinedurchsuchung gemäß § 100b StPO vergleichbar?

Auf die Antwort zu Frage 7 wird verwiesen.

12. Liegen nach Kenntnis der Bundesregierung bereits gerichtliche Entscheidungen vor, die sich mit der Zulässigkeit des Zugriffs auf die Daten von vernetzten Geräten durch die Strafverfolgungsbehörden auseinandergesetzt haben?

Der Bundesregierung sind keine gerichtlichen Entscheidungen bekannt, die sich mit der Zulässigkeit des Zugriffs auf die Daten von vernetzten Geräten durch die Strafverfolgungsbehörden auseinandergesetzt haben.

13. Unter welchen Voraussetzungen, aufgrund welcher bereits bestehender rechtlicher Grundlagen und in welchem Umfang ist Deutschland nach Ansicht der Bundesregierung verpflichtet im Rahmen internationaler Amtshilfe durch vernetzte Geräte aufgezeichnete und gespeicherte Daten an andere Staaten herauszugeben?

    Wie viele Anfragen sind der Bundesregierung in diesem Bereich bekannt?

    Wie wurde mit den jeweiligen Anfragen nach Kenntnis der Bundesregierung verfahren?

Für die Herausgabe von durch vernetzte Geräte aufgezeichnete und gespeicherte Daten durch deutsche Strafverfolgungsbehörden im Wege der internationalen Rechtshilfe gelten die allgemeinen, für den Bereich der internationalen Rechtshilfe maßgeblichen Vorschriften. Internationale Rechtshilfe wird demgemäß auf Grundlage und unter den Voraussetzungen des Gesetzes über die internationale Rechtshilfe in Strafsachen (IRG) und/oder internationaler Rechtshilfeabkommen in dem dort jeweils vorgesehenen Umfang geleistet. Der Bundesregierung sind keine Rechtshilfeersuchen bekannt, die sich auf die Herausgabe von durch vernetzte Geräte aufgezeichnete und gespeicherte Daten an Strafverfolgungsbehörden eines anderen Staates beziehen würden.

14. Inwiefern und in welchem Umfang unterfallen (lokal oder in der Cloud) gespeicherte Aufzeichnungen und Transkribierungen dieser Aufzeichnungen vernetzter Geräte nach Ansicht der Bundesregierung dem US-amerikanischen CLOUD Act?

Nach Auffassung der Bundesregierung können Daten und Transkribierungen der vernetzten Geräte dem US-amerikanischen CLOUD Act unterfallen, wenn es sich bei dem Anbieter der Leistung bzw. des vernetzten Geräts um ein US-amerikanisches Unternehmen handelt.

15. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes (GG) vereinbar?

16. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG vereinbar?

17. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Grundrecht des Fernmeldegeheimnisses aus Artikel 10 Absatz 1 GG vereinbar?

18. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Grundrecht auf Unverletzlichkeit der Wohnung gemäß Artikel 13 Absatz 1 GG vereinbar?

Die Fragen 15 bis 18 werden gemeinsam beantwortet.

Für die Zugriffsmöglichkeiten auf vernetzte Geräte gelten die allgemeinen Bestimmungen der StPO. Besonderheiten bei der Beurteilung der Verfassungsmäßigkeit ergeben sich daher nicht.

19. Wie ist aus Sicht der Bundesregierung der Zugriff von Strafverfolgungsbehörden auf die Daten vernetzter Geräte mit dem Recht, dass sich ein Beschuldigter nicht selbst belasten muss, vereinbar?

Nach dem nemo tenetur-Grundsatz ist niemand verpflichtet, zu seiner Strafverfolgung durch aktives Handeln beizutragen. Der Zugriff auf vernetzte Geräte im Rahmen und in den Grenzen der allgemeinen Vorschriften der StPO begründet eine solche Verpflichtung nicht.

20. Inwieweit nimmt nach Ansicht der Bundesregierung die Tiefe des Eingriffs durch den Umstand zu, dass es sich um einen Zugriff auf Alltagsgeräte und die von ihnen erfassten Informationen, die oftmals den privaten Lebensbereich der Bürgerinnen und der Bürger betreffen, handelt?

Die Tiefe des Eingriffs richtet sich nicht nach dem Gegenstand, sondern nach der Art Informationen, auf die zugegriffen wird. Eine besonders hohe Eingriffstiefe liegt vor, wenn ein Eingriff den Kernbereich der privaten Lebensführung betrifft. Mit § 100d StPO wurde durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl I, S. 3202 – 3213) daher eine Vorschrift geschaffen, die bei der Vornahme der Ermittlungsmaßnahmen nach den §§ 100a bis 100c den Schutz des Kernbereichs privater Lebensgestaltung sicherstellt.

21. Inwieweit ist die Bundesregierung der Ansicht, dass durch Zunahme der Möglichkeiten der Überwachung die Bürgerinnen und Bürger ein „diffus bedrohliches Gefühl des Beobachtetseins“ entwickeln könnten (vgl. BVerfG, Urteil des Ersten Senats vom 2. März 2010 – 1 BvR 256/08 – Rn. 1 – 345)?

Die Bundesregierung ist nicht dieser Ansicht.

22. Wie bewertet die Bundesregierung die Aussage des Bundesdatenschutzbeauftragten Ulrich Kelber, dass es sich bei dem Vorstoß um eine verfassungsrechtlich bedenkliche Kompetenzerweiterung handle (vgl. www.zdf.de/nachrichten/heute/innenminister-vorstoss-ermittler-sollen-zugriff-auf-daten-aus-smarten-geraeten-erhalten-100.html)?

Die Bundesregierung hat die Äußerung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zur Kenntnis genommen. Der BfDI ist unabhängig, eine Bewertung seiner Arbeit wird durch die Bundesregierung nicht vorgenommen. In faktischer Hinsicht ist richtigzustellen, dass – anders als in der zitierten Berichterstattung unzutreffend ausgeführt – die Bundesregierung nicht die Auffassung vertritt, dass es sich bei den in Rede stehenden vernetzten Geräten um eine neue Geräteklasse handele, die vom bestehenden Rechtsrahmen nicht umfasst sei.

23. Wie ist aus Sicht der Bundesregierung der Umstand verfassungsrechtlich zu bewerten, dass in einem Datensatz eines vernetzten Gerätes grundsätzlich auch eine Vielzahl von Daten unbeteiligter Dritter gespeichert sind, auf die die Strafverfolgungsbehörden ebenfalls zugreifen könnten?

Bei dem von den Fragestellern erörterten Phänomen handelt es sich nicht um ein neues Phänomen. Die bestehenden Eingriffsbefugnisse tragen dem bekannten Problem einer möglichen Mitbetroffenheit Dritter bei Ermittlungsmaßnahmen bereits hinreichend Rechnung.

24. Wie bewertet die Bundesregierung die Aussagekraft von Daten von vernetzten Geräten angesichts der Manipulierbarkeit dieser Daten etwa durch Hackerangriffe?

25. Welche Schlussfolgerungen zieht die Bundesregierung aus der Manipulierbarkeit der Daten von vernetzten Geräten für ihren Beweiswert vor Gericht?

Die Fragen 24 und 25 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Bezogen auf Strafverfahren obliegt die Beweiswürdigung im Einzelfall gemäß § 261 StPO dem Gericht. Eine Notwendigkeit gesonderter Regelungen ist nicht ersichtlich.

26. Für die Aufklärung welcher Straftatbestände kommt aus Sicht der Bundesregierung eine Ermächtigung der Strafverfolgungsbehörden, auf die Daten vernetzter Geräte zuzugreifen, in Betracht?

Die Maßnahme kann grundsätzlich bei allen Straftaten in Betracht kommen, soweit es sich um beweiserhebliche Daten handelt. § 110 Absatz 3 StPO setzt für den Zugriff auf räumlich getrennte Speichermedien zudem voraus, dass andernfalls der Verlust der gesuchten Daten zu besorgen ist. Dabei kommt es auf die rechtlichen und tatsächlichen Umstände des Einzelfalles an.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333